

(19) 日本国特許庁 (J-P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-301492

(43) 公開日 平成10年(1998)11月13日

(51) Int.Cl.⁸

G 0 9 C 1/00

識別記号

6 3 0

F I

G 0 9 C 1/00

6 3 0 D

6 3 0 C

6 3 0 E

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 C

6 0 1 E

審査請求 未請求 請求項の数17 O L (全 24 頁)

(21) 出願番号

特願平9-106136

(22) 出願日

平成9年(1997)4月23日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 石黒 隆二

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 刑部 義雄

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 弁理士 稲本 義雄

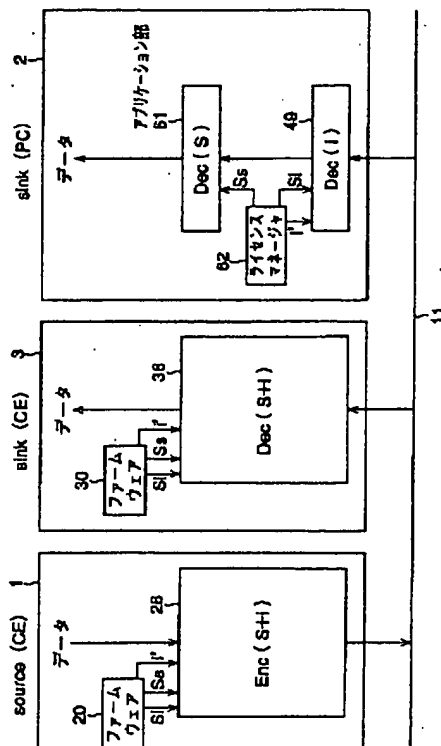
最終頁に続く

(54) 【発明の名称】 暗号化装置および方法、復号装置および方法、並びに情報処理装置および方法

(57) 【要約】

【課題】 不正なコピーを確実に防止する。

【解決手段】 DVDプレーヤ1の1394インタフェース26で暗号化されたデータを、1394バス11を介して、パーソナルコンピュータ2と光磁気ディスク装置3に伝送する。機能を変更することがユーザに開放されていない光磁気ディスク装置3においては、受信したデータを1394インタフェース36で復号する。これに対して、機能の変更がユーザに開放されているパーソナルコンピュータ2においては、1394インタフェース49で時変キーiを用いて暗号化データを復号し、その復号結果をアプリケーション部61でセッションキーSを用いてさらに復号する。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 暗号鍵を用いてデータを暗号化する暗号化手段と、

第1の鍵を発生する第1の発生手段と、
データを暗号化しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生手段と、
前記第1の鍵と第2の鍵を用いて前記暗号鍵を生成する生成手段とを備えることを特徴とする暗号化装置。

【請求項2】 前記生成手段は、準同形の暗号鍵を生成することを特徴とする請求項1に記載の暗号化装置。

【請求項3】 前記生成手段は、暗号化されたデータを、前記暗号鍵を構成する第1の暗号鍵と第2の暗号鍵を個別に用いて順次復号しても、正しい復号結果が得られる暗号鍵を生成することを特徴とする請求項1に記載の暗号化装置。

【請求項4】 前記生成手段は、前記第1の鍵を初期値とする値に、前記第2の鍵を加算して、前記暗号鍵を生成することを特徴とする請求項1に記載の暗号化装置。

【請求項5】 前記第1の鍵は、前記第2の鍵よりビット数が多く、
前記生成手段は、前記第2の鍵を、前記第1の鍵の所定の位置のビットに加算し、加算結果の所定の位置のビットを抽出し、抽出したビットをさらに加算して前記暗号鍵を生成することを特徴とする請求項4に記載の暗号化装置。

【請求項6】 前記生成手段は、前記抽出したビットをさらに加算して得た結果で、前記加算結果の所定のビットをさらに更新することを特徴とする請求項5に記載の暗号化装置。

【請求項7】 前記生成手段は、前記抽出したビットをさらに加算して得た結果の中から所定のものを、さらに所定のタイミングで選択して、前記暗号鍵を生成することを特徴とする請求項6に記載の暗号化装置。

【請求項8】 前記暗号鍵で暗号化したデータをバスを介して他の装置に伝送する伝送手段をさらに備えることを特徴とする請求項1に記載の暗号化装置。

【請求項9】 暗号鍵を用いてデータを暗号化する暗号化ステップと、

第1の鍵を発生する第1の発生ステップと、
データを暗号化しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生ステップと、
前記第1の鍵と第2の鍵を用いて前記暗号鍵を生成する生成ステップとを備えることを特徴とする暗号化方法。

【請求項10】 暗号化されているデータを受信する受信手段と、

前記受信したデータを、暗号鍵を用いて復号する復号手段と、

第1の鍵を発生する第1の発生手段と、
データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生手段と、

前記第1の鍵と第2の鍵を用いて前記暗号鍵を生成する生成手段とを備えることを特徴とする復号装置。

【請求項11】 前記生成手段は、

前記第1の鍵と第2の鍵の一方を用いて第1の暗号鍵を生成する第1の生成手段と、

前記第1の鍵と第2の鍵の他方を用いて第2の暗号鍵を生成する第2の生成手段とを備え、

前記復号手段は、

前記第1の暗号鍵を用いて、前記暗号化されているデータを復号する第1の復号手段と、

前記第1の復号手段により復号されたデータを、前記第2の暗号鍵を用いて、さらに復号する第2の復号手段とを備えることを特徴とする請求項10に記載の復号装置。

【請求項12】 前記第2の復号手段は、復号されたデータを処理するアプリケーションソフトウェアにより構成されることを特徴とする請求項11に記載の復号装置。

【請求項13】 暗号化されているデータを受信する受信ステップと、

前記受信したデータを、暗号鍵を用いて復号する復号ステップと、

第1の鍵を発生する第1の発生ステップと、

データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生ステップと、

前記第1の鍵と第2の鍵を用いて前記暗号鍵を生成する生成ステップとを備えることを特徴とする復号方法。

【請求項14】 バスを介して相互に接続された複数の情報処理装置により構成される情報処理システムにおいて、

前記情報処理装置は、

機能の変更がユーザに開放されていない第1の情報処理装置と、

機能の変更がユーザに開放されている第2の情報処理装置とにより構成され、

前記第1の情報処理装置は、

暗号化されているデータを受信する第1の受信手段と、
前記第1の受信手段が受信したデータを、暗号鍵を用いて復号する第1の復号手段と、

第1の鍵を発生する第1の発生手段と、

データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生手段と、

前記第1の発生手段が発生する第1の鍵と前記第2の発生手段が発生する第2の鍵を用いて前記暗号鍵を生成する第1の生成手段とを備え、

前記第2の情報処理装置は、

暗号化されているデータを受信する第2の受信手段と、

前記第1の鍵を発生する第3の発生手段と、

データを復号しているとき、所定のタイミングで変更される前記第2の鍵を発生する第4の発生手段と、

前記第3の発生手段が発生する第1の鍵と前記第4の発生手段が発生する第2の鍵の一方を用いて第1の暗号鍵を生成する第2の生成手段と、

前記第3の発生手段が発生する第1の鍵と前記第4の発生手段が発生する第2の鍵の他方を用いて第2の暗号鍵を生成する第3の生成手段と、

前記第1の暗号鍵を用いて、前記受信手段が受信した、暗号化されているデータを復号する第2の復号手段と、前記第2の復号手段により復号されたデータを、前記第2の暗号鍵を用いて、さらに復号する第3の復号手段とを備えることを特徴とする情報処理システム。

【請求項15】 バスを介して相互に接続された複数の情報処理装置により構成される情報処理システムの情報処理方法において、

前記情報処理装置は、

機能の変更がユーザに開放されていない第1の情報処理装置と、

機能の変更がユーザに開放されている第2の情報処理装置とにより構成され、

前記第1の情報処理装置は、

暗号化されているデータを受信する第1の受信ステップと、

前記第1の受信ステップで受信したデータを、暗号鍵を用いて復号する第1の復号ステップと、

第1の鍵を発生する第1の発生ステップと、

データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生ステップと、

前記第1の発生ステップで発生する第1の鍵と前記第2の発生ステップで発生する第2の鍵を用いて前記暗号鍵を生成する第1の生成ステップとを備え、

前記第2の情報処理装置は、

暗号化されているデータを受信する第2の受信ステップと、

前記第1の鍵を発生する第3の発生ステップと、

データを復号しているとき、所定のタイミングで変更される前記第2の鍵を発生する第4の発生ステップと、

前記第3の発生ステップで発生する第1の鍵と前記第4の発生ステップで発生する第2の鍵の一方を用いて第1の暗号鍵を生成する第2の生成ステップと、

前記第3の発生ステップで発生する第1の鍵と前記第4の発生ステップで発生する第2の鍵の他方を用いて第2の暗号鍵を生成する第3の生成ステップと、

前記第1の暗号鍵を用いて、前記第2の受信ステップで受信した、暗号化されているデータを復号する第2の復号ステップと、

前記第2の復号ステップで復号されたデータを、前記第2の暗号鍵を用いて、さらに復号する第3の復号ステップとを備えることを特徴とする情報処理方法。

【請求項16】 バスを介して伝送されてきたデータを受信する受信手段と、

前記受信手段が受信したデータから、第1の暗号鍵と、データを復号しているとき、所定のタイミングで変更される第2の暗号鍵を生成する、ソフトウェアプログラムからなる生成手段と、

前記生成手段が生成した第1の暗号鍵と第2の暗号鍵の一方を用いて、前記受信手段が受信した、暗号化されているデータを復号する第1の復号手段と、

前記第1の復号手段により復号されたデータを、前記生成手段が生成した第1の暗号鍵と第2の暗号鍵の他方を用いて、さらに復号して処理する、ソフトウェアプログラムからなる第2の復号手段とを備えることを特徴とする情報処理装置。

【請求項17】 バスを介して伝送されてきたデータを受信する受信ステップと、

前記受信ステップで受信したデータから、第1の暗号鍵と、データを復号しているとき、所定のタイミングで変更される第2の暗号鍵を生成する、ソフトウェアプログラムからなる生成ステップと、

前記生成ステップで生成した第1の暗号鍵と第2の暗号鍵の一方を用いて、前記受信ステップで受信した、暗号化されているデータを復号する第1の復号ステップと、前記第1の復号ステップで復号されたデータを、前記生成ステップで生成した第1の暗号鍵と第2の暗号鍵の他方を用いて、さらに復号して処理する、ソフトウェアプログラムからなる第2の復号ステップとを備えることを特徴とする情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号化装置および方法、復号装置および方法、並びに情報処理装置および方法に関し、特に、より安全性を高めるようにした暗号化装置および方法、復号装置および方法、並びに情報処理装置および方法に関する。

【0002】

【従来の技術】最近、AV機器、コンピュータなどに代表される複数の電子機器を、バスで相互に接続し、ネットワークを構成して、ネットワーク内で各種のデータを相互に授受することができるようになってきた。

【0003】その結果、例えば、ネットワークに接続されているDVDプレーヤにより、DVDから再生した映画のデータを、バスを介して、テレビジョン受像機、モニタなどの表示装置に転送し、表示することができる。通常、DVDより再生された映画を表示装置に表示して視聴することは、DVDを購入した時点において、著作権者から許容されるところである。

【0004】しかしながら、DVDから再生されたデータを、他の記録媒体にコピーし、利用することは、一般的には著作権者から許容されていない。そこで、バス（ネットワーク）を介して送出するデータが、不法にコピーされるのを防止するために、送出する側において、デー

データを暗号化するようにし、受信側において、これを復号することが考えられる。

【0005】しかしながら、DVDプレーヤ、テレビジョン受像機などのコンシューマエレクトロニクス機器（CE機器）は、通常、所定の目的のために設計、製造されているものであり、ユーザがこれを改造したり、他の部品を組み込んだりして、装置の内部のデータを取得したり、改ざんしたりすること（機能の変更）はできないように製造されている。これに対して、例えばパーソナルコンピュータは、多くの場合、アーキテクチャや回路が公開されており、ボードなどを追加したり、各種のアプリケーションソフトウェアをインストールすることにより、様々な機能を追加、変更することができるようになされている。

【0006】従って、パーソナルコンピュータにおいては、その内部バス上のデータを、所定のハードウェアを付加したり、ソフトウェアプログラムを作成することで、パーソナルコンピュータ内部のバス上のデータを直接見たり、改ざんすることが、比較的容易に行うことができる。このことは、例えば、DVDプレーヤからテレビジョン受像機に暗号化して伝送したデータを、パーソナルコンピュータで受け取り、これを復号して、コピーしたりすることが、アプリケーションソフトウェアを作成することで、容易に行えることを意味する。

【0007】換言すれば、パーソナルコンピュータは、バスを介して、通信を行うリンク部と、送受信するデータを用意したり、受信したデータを利用するアプリケーション部とのつながりが希薄であり、物理的にも、論理的にも、そこにユーザが手を加えることができる部分が多い。これに対して、CE機器においては、両者のつながりが密接で、ユーザが介入できる部分が殆どない。

【0008】

【発明が解決しようとする課題】本発明はこのような状況に鑑みてなされたものであり、データの不正なコピーを、より確実に防止することができるようにするものである。

【0009】

【課題を解決するための手段】請求項1に記載の暗号化装置は、暗号鍵を用いてデータを暗号化する暗号化手段と、第1の鍵を発生する第1の発生手段と、データを暗号化しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生手段と、第1の鍵と第2の鍵を用いて暗号鍵を生成する生成手段とを備えることを特徴とする。

【0010】請求項9に記載の暗号化方法は、暗号鍵を用いてデータを暗号化する暗号化ステップと、第1の鍵を発生する第1の発生ステップと、データを暗号化しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生ステップと、第1の鍵と第2の鍵を用いて暗号鍵を生成する生成ステップとを備えることを特

徴とする。

【0011】請求項10に記載の復号装置は、暗号化されているデータを受信する受信手段と、受信したデータを、暗号鍵を用いて復号する復号手段と、第1の鍵を発生する第1の発生手段と、データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生手段と、第1の鍵と第2の鍵を用いて暗号鍵を生成する生成手段とを備えることを特徴とする。

【0012】請求項13に記載の復号方法は、暗号化されているデータを受信する受信ステップと、受信したデータを、暗号鍵を用いて復号する復号ステップと、第1の鍵を発生する第1の発生ステップと、データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生ステップと、第1の鍵と第2の鍵を用いて暗号鍵を生成する生成ステップとを備えることを特徴とする。

【0013】請求項14に記載の情報処理システムは、情報処理装置は、機能の変更がユーザに開放されていない第1の情報処理装置と、機能の変更がユーザに開放されている第2の情報処理装置とにより構成され、第1の情報処理装置は、暗号化されているデータを受信する第1の受信手段と、第1の受信手段が受信したデータを、暗号鍵を用いて復号する第1の復号手段と、第1の鍵を発生する第1の発生手段と、データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第2の発生手段と、第1の発生手段が発生する第1の鍵と第2の発生手段が発生する第2の鍵を用いて暗号鍵を生成する第1の生成手段とを備え、第2の情報処理装置は、暗号化されているデータを受信する第2の受信手段と、第1の鍵を発生する第3の発生手段と、データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第4の発生手段と、第3の発生手段が発生する第1の鍵と第4の発生手段が発生する第2の鍵の一方を用いて第1の暗号鍵を生成する第2の生成手段と、第3の発生手段が発生する第1の鍵と第4の発生手段が発生する第2の鍵の他方を用いて第2の暗号鍵を生成する第3の生成手段と、第1の暗号鍵を用いて、受信手段が受信した、暗号化されているデータを復号する第2の復号手段と、第2の復号手段により復号されたデータを、第2の暗号鍵を用いて、さらに復号する第3の復号手段とを備えることを特徴とする。

【0014】請求項15に記載の情報処理方法は、情報処理装置は、機能の変更がユーザに開放されていない第1の情報処理装置と、機能の変更がユーザに開放されている第2の情報処理装置とにより構成され、第1の情報処理装置は、暗号化されているデータを受信する第1の受信ステップと、第1の受信ステップで受信したデータを、暗号鍵を用いて復号する第1の復号ステップと、第1の鍵を発生する第1の発生ステップと、データを復号しているとき、所定のタイミングで変更される第2の鍵

を発生する第2の発生ステップと、第1の発生ステップで発生する第1の鍵と第2の発生ステップで発生する第2の鍵を用いて暗号鍵を生成する第1の生成ステップとを備え、第2の情報処理装置は、暗号化されているデータを受信する第2の受信ステップと、第1の鍵を発生する第3の発生ステップと、データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第4の発生ステップと、第3の発生ステップで発生する第1の鍵と第4の発生ステップで発生する第2の鍵の一方を用いて第1の暗号鍵を生成する第2の生成ステップと、第3の発生ステップで発生する第1の鍵と第4の発生ステップで発生する第2の鍵の他方を用いて第2の暗号鍵を生成する第3の生成ステップと、第1の暗号鍵を用いて、第2の受信ステップで受信した、暗号化されているデータを復号する第2の復号ステップと、第2の復号ステップで復号されたデータを、第2の暗号鍵を用いて、さらに復号する第3の復号ステップとを備えることを特徴とする。

【0015】請求項16に記載の情報処理装置は、バスを介して伝送されてきたデータを受信する受信手段と、受信手段が受信したデータから、第1の暗号鍵と、データを復号しているとき、所定のタイミングで変更される第2の暗号鍵を生成する、ソフトウェアプログラムからなる生成手段と、生成手段が生成した第1の暗号鍵と第2の暗号鍵の一方を用いて、受信手段が受信した、暗号化されているデータを復号する第1の復号手段と、第1の復号手段により復号されたデータを、生成手段が生成した第1の暗号鍵と第2の暗号鍵の他方を用いて、さらに復号して処理する、ソフトウェアプログラムからなる第2の復号手段とを備えることを特徴とする。

【0016】請求項17に記載の情報処理方法は、バスを介して伝送されてきたデータを受信する受信ステップと、受信ステップで受信したデータから、第1の暗号鍵と、データを復号しているとき、所定のタイミングで変更される第2の暗号鍵を生成する、ソフトウェアプログラムからなる生成ステップと、生成ステップで生成した第1の暗号鍵と第2の暗号鍵の一方を用いて、受信ステップで受信した、暗号化されているデータを復号する第1の復号ステップと、第1の復号ステップで復号されたデータを、生成ステップで生成した第1の暗号鍵と第2の暗号鍵の他方を用いて、さらに復号して処理する、ソフトウェアプログラムからなる第2の復号ステップとを備えることを特徴とする。

【0017】請求項1に記載の暗号化装置および請求項9に記載の暗号化方法においては、第1の鍵と、データを暗号化しているとき、所定のタイミングで変更される第2の鍵を用いて暗号鍵が生成される。

【0018】請求項10に記載の復号装置および請求項13に記載の復号方法においては、第1の鍵と、データを復号しているとき、所定のタイミングで変更される第

2の鍵を用いて暗号鍵が生成される。

【0019】請求項14に記載の情報処理システムおよび請求項15に記載の情報処理方法においては、機能の変更がユーザに開放されていない第1の情報処理装置においては、第1の鍵と、データを復号しているとき、所定のタイミングで変更される第2の鍵を用いて、暗号鍵が生成される。これに対して、機能の変更がユーザに開放されている第2の情報処理装置においては、第1の鍵と、データを復号しているとき、所定のタイミングで変更される第2の鍵の一方を用いて第1の暗号鍵が生成され、他方を用いて第2の暗号鍵が生成される。そして、第1の暗号鍵を用いて、暗号化されているデータが復号され、復号されたデータが、さらに第2の暗号鍵を用いて、さらに復号される。

【0020】請求項16に記載の情報処理装置および請求項17に記載の情報処理方法においては、受信したデータから、第1の暗号鍵と、データを復号しているとき、所定のタイミングで変更される第2の暗号鍵が、ソフトウェアプログラムで生成される。

【0021】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0022】請求項1に記載の暗号化装置は、暗号鍵を用いてデータを暗号化する暗号化手段（例えば図12の加算器74）と、第1の鍵（例えば初期値キーSs）を発生する第1の発生手段（例えば図12の加算器81）と、データを暗号化しているとき、所定のタイミングで変更される第2の鍵（例えばキーi）を発生する第2の発生手段（例えば図12の加算器86）と、第1の鍵と第2の鍵を用いて暗号鍵（例えば図12のシュリンクジェネレータ73の出力）を生成する生成手段（例えば図12のアディティブジェネレータ71、LFSR72、シュリンクジェネレータ73）とを備えることを特徴とする。

【0023】請求項8に記載の暗号化装置は、暗号鍵で暗号化したデータをバスを介して他の装置に伝送する伝送手段（例えば図2の1394インタフェース26）をさらに備えることを特徴とする。

【0024】請求項10に記載の復号装置は、暗号化されているデータを受信する受信手段（例えば図2の1394インタフェース49）と、受信したデータを、暗号鍵を用いて復号する復号手段（例えば図16の減算器174）と、第1の鍵（例えば初期値キーSs）を発生する第1の発生手段（例えば図16の加算器181）と、データを復号しているとき、所定のタイミングで変更され

る第2の鍵(例えばキーi)を発生する第2の発生手段(例えば図16の加算器186)と、第1の鍵と第2の鍵を用いて暗号鍵を生成する生成手段(例えば図16のアディティブジェネレータ171、LFSR172、シュリンクジェネレータ173)とを備えることを特徴とする。

【0025】請求項11に記載の復号装置は、生成手段は、第1の鍵と第2の鍵の一方を用いて第1の暗号鍵を生成する第1の生成手段(例えば図18の加算器283)と、第1の鍵と第2の鍵の他方を用いて第2の暗号鍵を生成する第2の生成手段(例えば図20の加算器383)とを備え、復号手段は、第1の暗号鍵を用いて、暗号化されているデータを復号する第1の復号手段(例えば図18の減算器274)と、第1の復号手段により復号されたデータを、第2の暗号鍵を用いて、さらに復号する第2の復号手段(例えば図20の減算器374)とを備えることを特徴とする。

【0026】請求項14に記載の情報処理システムは、情報処理装置は、機能の変更がユーザに開放されていない第1の情報処理装置(例えば図2の光磁気ディスク装置3)と、機能の変更がユーザに開放されている第2の情報処理装置(例えば図2のパーソナルコンピュータ2)とにより構成され、第1の情報処理装置は、暗号化されているデータを受信する第1の受信手段(例えば図2の1394インタフェース36)と、第1の受信手段が受信したデータを、暗号鍵を用いて復号する第1の復号手段(例えば図16の減算器174)と、第1の鍵

(例えば初期値キーSs)を発生する第1の発生手段(例えば図16の加算器181)と、データを復号しているとき、所定のタイミングで変更される第2の鍵(例えばキーi)を発生する第2の発生手段(例えば図16の加算器186)と、第1の発生手段が発生する第1の鍵と第2の発生手段が発生する第2の鍵を用いて暗号鍵を生成する第1の生成手段(例えば図16のアディティブジェネレータ171)とを備え、第2の情報処理装置は、暗号化されているデータを受信する第2の受信手段(例えば図2の1394インタフェース49)と、第1の鍵を発生する第3の発生手段(例えば図18の加算器281)と、データを復号しているとき、所定のタイミングで変更される第2の鍵を発生する第4の発生手段(例えば図18の加算器286)と、第3の発生手段が発生する第1の鍵と第4の発生手段が発生する第2の鍵の一方を用いて第1の暗号鍵を生成する第2の生成手段(例えば図18のアディティブジェネレータ271)と、第3の発生手段が発生する第1の鍵と第4の発生手段が発生する第2の鍵の他方を用いて第2の暗号鍵を生成する第3の生成手段(例えば図20のアディティブジェネレータ371)と、第1の暗号鍵を用いて、受信手段が受信した、暗号化されているデータを復号する第2の復号手段(例えば図20の減算器374)と、第2の復号手段

により復号されたデータを、第2の暗号鍵を用いて、さらに復号する第3の復号手段(例えば図20の減算器374)とを備えることを特徴とする。

【0027】請求項16に記載の情報処理装置は、バスを介して伝送されてきたデータを受信する受信手段(例えば図10の1394インタフェース49)と、受信手段が受信したデータから、第1の暗号鍵と、データを復号しているとき、所定のタイミングで変更される第2の暗号鍵を生成する、ソフトウェアプログラムからなる生成手段(例えば図10のライセンスマネージャ62)と、生成手段が生成した第1の暗号鍵と第2の暗号鍵の一方を用いて、受信手段が受信した、暗号化されているデータを復号する第1の復号手段(例えば図10の1394インタフェース49)と、第1の復号手段により復号されたデータを、生成手段が生成した第1の暗号鍵と第2の暗号鍵の他方を用いて、さらに復号して処理する、ソフトウェアプログラムからなる第2の復号手段(例えば図10のアプリケーション部61)とを備えることを特徴とする。

【0028】図1は、本発明を適用した情報処理システムの構成例を表している。この構成例においては、IEEE1394シリアルバス11を介してDVDプレーヤ1、パーソナルコンピュータ2、光磁気ディスク装置3、データ放送受信装置4、モニタ5、テレビジョン受像機6が相互に接続されている。

【0029】図2は、この内のDVDプレーヤ1、パーソナルコンピュータ2、および光磁気ディスク装置3の内部のより詳細な構成例を表している。DVDプレーヤ1は、1394インタフェース26を介して、1394バス11に接続されている。CPU21は、ROM22に記憶されているプログラムに従って各種の処理を実行し、RAM23は、CPU21が各種の処理を実行する上において必要なデータやプログラムなどを適宜記憶する。操作部24は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより操作されたとき、その操作に対応する信号を出力する。ドライブ25は、図示せぬDVD(ディスク)を駆動し、そこに記録されているデータを再生するようになされている。EEPROM27は、装置の電源オフ後も記憶する必要のある情報(この実施の形態の場合、鍵情報)を記憶するようになされている。内部バス28は、これらの各部を相互に接続している。

【0030】光磁気ディスク装置3は、CPU31乃至内部バス38を有している。これらは、上述したDVDプレーヤ1におけるCPU21乃至内部バス28と同様の機能を有するものであり、その説明は省略する。ただし、ドライブ35は、図示せぬ光磁気ディスクを駆動し、そこにデータを記録または再生するようになされている。

【0031】パーソナルコンピュータ2は、1394インタフェース49を介して1394バス11に接続されている。CPU41は、ROM42に記憶されているプログラ

ムに従って各種の処理を実行する。RAM 4 3には、CPU 4 1が各種の処理を実行する上において必要なデータやプログラムなどが適宜記憶される。入出力インタフェース 4 4には、キーボード 4 5とマウス 4 6が接続されており、それらから入力された信号をCPU 4 1に出力するようになされている。また、入出力インタフェース 4 4には、ハードディスク (HDD) 4 7が接続されており、そこにデータ、プログラムなどを記録再生することができるようになされている。入出力インタフェース 4 4にはまた、拡張ボード 4 8を適宜装着し、必要な機能を付加

【0032】なお、この内部バス 5 1は、ユーザに対して解放されており、ユーザは、拡張ボード 4 8に所定のボードを適宜接続したり、所定のソフトウェアプログラムを作成して、CPU 4 1にインストールすることで、内部バス 5 1により伝送されるデータを適宜受信することができるようになされている。

【0033】これに対して、DVDプレーヤ 1や光磁気ディスク装置 3などのコンシューマエレクトロニクス (CE) 装置においては、内部バス 2 8や内部バス 3 8は、ユーザに解放されておらず、特殊な改造などを行わない限り、そこに伝送されるデータを取得することができないようになされている。

【0034】次に、所定のソースとシンクとの間で行われる認証の処理について説明する。この認証の処理は、図 3に示すように、ソースとしての、例えばDVDプレーヤ 1のROM 2 2に予め記憶されているソフトウェアプログラムの1つとしてのファームウェア 2 0と、シンクとしての、例えばパーソナルコンピュータ 2のROM 4 2に記憶されており、CPU 4 1が処理するソフトウェアプログラムの1つとしてのライセンスマネージャ 6 2との間において行われる。

【0035】図 4は、ソース (DVDプレーヤ 1) と、シンク (パーソナルコンピュータ 2) との間において行われる認証の手順を示している。DVDプレーヤ 1のEEPROM 2 7には、サービスキー (service_key) と関数 (hash) が予め記憶されている。これらはいずれも著作権者から、このDVDプレーヤ 1のユーザに与えられたものであり、各ユーザは、EEPROM 2 7に、これを秘密裡に保管しておくものである。

【0036】サービスキーは、著作権者が提供する情報毎に与えられるものであり、この1394バス 1 1で構成されるシステムにおいて、共通のものである。なお、本明細書において、システムとは、複数の装置で構成さ

れる全体的な装置を示すものとする。

【0037】hash関数は、任意長の入力に対して、64ビットまたは128ビットなどの固定長のデータを出力する関数であり、 $y (=hash(x))$ を与えられたとき、 x を求めることが困難であり、かつ、 $hash(x1) = hash(x2)$ となる $x1$ と、 $x2$ の組を求めることも困難となる関数である。1方向hash関数の代表的なものとして、MD5やSHAなどが知られている。この1方向hash関数については、BruceSchneier著の「Applied Cryptography (Second Edition), Wiley」に詳しく解説されている。

【0038】一方、シンクとしての例えばパーソナルコンピュータ 2は、著作権者から与えられた、自分自身に固有の識別番号 (ID) とライセンスキー (license_key) をEEPROM 5 0に秘密裡に保持している。このライセンスキーは、 n ビットのIDと m ビットのサービスキーを連結して得た $n+m$ ビットのデータ (ID || service_key) に対して、hash関数を適用して得られる値である。すなわち、ライセンスキーは次式で表される。

licence_key=hash(ID || service_key)

【0039】IDとしては、例えば1394バス 1 1の規格に定められているnode_unique_IDを用いることができる。このnode_unique_IDは、図 5に示すように、8バイト (64ビット) で構成され、最初の3バイトは、IEEEで管理され、電子機器の各メーカーにIEEEから付与される。また、下位5バイトは、各メーカーが、自分自身がユーザに提供する各装置に対して付与することができるものである。各メーカーは、例えば下位5バイトに対してシリアルに、1台に1個の番号を割り当てるようにし、5バイト分を全部使用した場合には、上位3バイトがさらに別の番号となっているnode_unique_IDの付与を受け、そして、その下位5バイトについて1台に1個の番号を割り当てるようにする。従って、このnode_unique_IDは、メーカーに拘らず、1台毎に異なるものとなり、各装置に固有のものとなる。

【0040】ステップ S 1において、DVDプレーヤ 1のファームウェア 2 0は、1394インタフェース 2 6を制御し、1394バス 1 1を介してパーソナルコンピュータ 2に対してIDを要求する。パーソナルコンピュータ 2のライセンスマネージャ 6 2は、ステップ S 2において、このIDの要求を受信する。すなわち、1394インタフェース 4 9は、1394バス 1 1を介してDVDプレーヤ 1から伝送されてきたID要求の信号を受信すると、これをCPU 4 1に出力する。CPU 4 1のライセンスマネージャ 6 2は、このID要求を受けたとき、ステップ S 3においてEEPROM 5 0に記憶されているIDを読み出し、これを1394インタフェース 4 9を介して1394バス 1 1からDVDプレーヤ 1に伝送する。

【0041】DVDプレーヤ 1においては、ステップ S 4で1394インタフェース 2 6が、このIDを受け取る

と、このIDがCPU 21で動作しているファームウェア20に供給される。

【0042】ファームウェア20は、ステップS5において、パーソナルコンピュータ2から伝送を受けたIDと、EEPROM 27に記憶されているサービスキーを結合して、データ (ID || service_key) を生成し、このデータに対して、次式に示すようにhash関数を適用して、キーlkを生成する。

$lk = \text{hash} (ID || \text{service_key})$

【0043】次に、ステップS6において、ファームウェア20は、暗号鍵skを生成する。この暗号鍵skの詳細については後述するが、この暗号鍵skは、セッションキーとしてDVDプレーヤ1とパーソナルコンピュータ2のそれぞれにおいて利用される。

【0044】次に、ステップS7において、ファームウェア20は、ステップS5で生成した鍵lkを鍵として、ステップS6で生成した暗号鍵skを暗号化して、暗号化データ (暗号化鍵) eを得る。すなわち、次式を演算する。

$e = \text{Enc} (lk, sk)$

【0045】なお、Enc (A, B) は、共通鍵暗号方式で、鍵Aを用いて、データBを暗号化することを意味する。

【0046】次に、ステップS8で、ファームウェア20は、ステップS7で生成した暗号化データeをパーソナルコンピュータ2に伝送する。すなわち、この暗号化データeは、DVDプレーヤ1の1394インタフェース26から1394バス11を介してパーソナルコンピュータ2に伝送される。パーソナルコンピュータ2においては、ステップS9で、この暗号化データeを1394インタフェース49を介して受信する。ライセンスマネージャ62は、このようにして受信した暗号化データeをEEPROM 50に記憶されているライセンスキーを鍵として、次式に示すように復号し、復号鍵sk'を生成する。

$sk' = \text{Dec} (\text{license_key}, e)$

【0047】なお、ここで、Dec (A, B) は、共通鍵暗号方式で鍵Aを用いて、データBを復号することを意味する。

【0048】なお、この共通鍵暗号方式における暗号化のアルゴリズムとしては、DESが知られている。共通鍵暗号化方式についても、上述した、Applied Cryptography (Second Edition) に詳しく解説されている。

【0049】DVDプレーヤ1において、ステップS5で生成するキーlkは、パーソナルコンピュータ2のEEPROM 50に記憶されている (license_key) と同一の値となる。すなわち、次式が成立する。

$lk = \text{license_key}$

【0050】従って、パーソナルコンピュータ2において、ステップS10で復号して得たキーsk'は、DVDプレーヤ1において、ステップS6で生成した暗号鍵skと同

一の値となる。すなわち、次式が成立する。 $sk' = sk$

【0051】このように、DVDプレーヤ1 (ソース) とパーソナルコンピュータ2 (シンク) の両方において、同一の鍵sk, sk'を共有することができる。そこで、この鍵skをそのまま暗号鍵として用いるか、あるいは、これを基にして、それぞれが疑似乱数を作り出し、それを暗号鍵として用いることができる。

【0052】ライセンスキーは、上述したように、各装置に固有のIDと、提供する情報に対応するサービスキーに基づいて生成されているので、他の装置がskまたはsk'を生成することはできない。また、著作権者から認められていない装置は、ライセンスキーを有していないので、skあるいはsk'を生成することができない。従って、その後DVDプレーヤ1が暗号鍵skを用いて再生データを暗号化してパーソナルコンピュータ2に伝送した場合、パーソナルコンピュータ2が適正にライセンスキーを得たものである場合には、暗号鍵sk'を有しているので、DVDプレーヤ1より伝送されてきた、暗号化されている再生データを復号することができる。しかしながら、パーソナルコンピュータ2が適正なものでない場合、暗号鍵sk'を有していないので、伝送されてきた暗号化されている再生データを復号することができない。換言すれば、適正な装置だけが共通の暗号鍵sk, sk'を生成することができるので、結果的に、認証が行われることになる。

【0053】仮に1台のパーソナルコンピュータ2のライセンスキーが盗まれたとしても、IDが1台1台異なるので、そのライセンスキーを用いて、他の装置がDVDプレーヤ1から伝送されてきた暗号化されているデータを復号することはできない。従って、安全性が向上する。

【0054】図6は、ソース (DVDプレーヤ1) に対して、パーソナルコンピュータ2だけでなく、光磁気ディスク装置3もシンクとして機能する場合の処理例を表している。

【0055】この場合、シンク1としてのパーソナルコンピュータ2のEEPROM 50には、IDとしてID1が、また、ライセンスキーとしてlicense_key1が記憶されており、シンク2としての光磁気ディスク装置3においては、EEPROM 37に、IDとしてID2が、また、ライセンスキーとしてlicense_key2が記憶されている。

【0056】DVDプレーヤ1 (ソース) とパーソナルコンピュータ2 (シンク1) の間において行われるステップS11乃至ステップS20の処理は、図4におけるステップS1乃至ステップS10の処理と実質的に同様の処理であるので、その説明は省略する。

【0057】すなわち、上述したようにして、DVDプレーヤ1は、パーソナルコンピュータ2に対して認証処理を行う。そして次に、ステップS21において、DVDプレーヤ1は、光磁気ディスク装置3に対して、IDを要求する。光磁気ディスク装置3においては、ステップS2

2で1394インタフェース36を介して、このID要求信号が受信されると、そのファームウェア30(図10)は、ステップS23でEEPROM37に記憶されているID(ID2)を読み出し、これを1394インタフェース36から、1394バス11を介してDVDプレーヤ1に伝送する。DVDプレーヤ1のファームウェア20は、ステップS24で、1394インタフェース26を介して、このID2を受け取ると、ステップS25で、次式から鍵lk2を生成する。

$lk2 = \text{hash}(ID2 \parallel service_key)$

【0058】さらに、ファームウェア20は、ステップS26で次式を演算し、ステップS16で生成した鍵skを、ステップS25で生成した鍵lk2を用いて暗号化し、暗号化したデータe2を生成する。

【0059】そして、ステップS27で、ファームウェア20は、この暗号化データe2を1394インタフェース26から1394バス11を介して光磁気ディスク装置3に伝送する。

【0060】光磁気ディスク装置3においては、ステップS28で1394インタフェース36を介して、この暗号化データe2を受信し、ステップS29で次式を演算して、暗号鍵sk2'を生成する。

$sk2' = \text{Dec}(license_key2, e2)$

【0061】以上のようにして、パーソナルコンピュータ2と光磁気ディスク装置3のそれぞれにおいて、暗号鍵sk1', sk2'が得られたことになる。これらの値は、DVDプレーヤ1における暗号鍵skと同一の値となっている。

【0062】図6の処理例においては、DVDプレーヤ1が、パーソナルコンピュータ2と、光磁気ディスク装置3に対して、それぞれ個別にIDを要求し、処理するようにしているのであるが、同報通信によりIDを要求することができる場合は、図7に示すような処理を行うことができる。

【0063】すなわち、図7の処理例においては、ステップS41で、ソースとしてのDVDプレーヤ1が、全てのシンク(この例の場合、パーソナルコンピュータ2と光磁気ディスク装置3)に対して同報通信でIDを要求する。パーソナルコンピュータ2と光磁気ディスク装置3は、それぞれステップS42とステップS43で、このID転送要求の信号を受け取ると、それぞれステップS44またはステップS45で、EEPROM50またはEEPROM37に記憶されているID1またはID2を読み出し、これをDVDプレーヤ1に転送する。DVDプレーヤ1は、ステップS46とステップS47で、これらのIDをそれぞれ受信する。

【0064】DVDプレーヤ1においては、さらにステップS48で、次式から暗号鍵lk1を生成する。

$lk1 = \text{hash}(ID1 \parallel service_key)$

【0065】さらに、ステップS49において、次式か

ら暗号鍵lk2が生成される。

$lk2 = \text{hash}(ID2 \parallel service_key)$

【0066】DVDプレーヤ1においては、さらにステップS50で、暗号鍵skが生成され、ステップS51で、次式で示すように、暗号鍵skが、鍵lk1を鍵として暗号化される。

$e1 = \text{Enc}(lk1, sk)$

【0067】さらに、ステップS52においては、暗号鍵skが、鍵lk2を鍵として、次式に従って暗号化される。

$e2 = \text{Enc}(lk2, sk)$

【0068】さらに、ステップS53においては、ID1, e1, ID2, e2が、それぞれ次式で示すように結合されて、暗号化データeが生成される。

$e = ID1 \parallel e1 \parallel ID2 \parallel e2$

【0069】DVDプレーヤ1においては、さらにステップS54で、以上のようにして生成された暗号化データeが同報通信で、パーソナルコンピュータ2と光磁気ディスク装置3に伝送される。

【0070】パーソナルコンピュータ2と光磁気ディスク装置3においては、それぞれステップS55またはステップS56で、これらの暗号化データeが受信される。そして、パーソナルコンピュータ2と光磁気ディスク装置3においては、それぞれステップS57またはステップS58において、次式で示す演算が行われ、暗号鍵sk1', sk2'が生成される。

$sk1' = \text{Dec}(license_key1, e1)$

$sk2' = \text{Dec}(license_key2, e2)$

【0071】図8は、1つのシンクが複数のサービスの受けること(複数の種類の情報の復号)ができるようになされている場合の処理例を表している。すなわち、この場合においては、例えば、シンクとしてのパーソナルコンピュータ2は、複数のライセンスキー(license_key1, license_key2, license_key3など)をEEPROM50に記憶している。ソースとしてのDVDプレーヤ1は、そのEEPROM27に複数のサービスキー(service_key1, service_key2, service_key3など)を記憶している。この場合、DVDプレーヤ1は、ステップS81でシンクとしてのパーソナルコンピュータ2に対してIDを要求するとき、DVDプレーヤ1が、これから転送しようとする情報(サービス)を識別するservice_IDを転送する。パーソナルコンピュータ2においては、ステップS82で、これを受信したとき、EEPROM50に記憶されている複数のライセンスキーの中から、このservice_IDに対応するものを選択し、これを用いて、ステップS90で復号処理を行う。その他の動作は、図4における場合と同様である。

【0072】図9は、さらに他の処理例を表している。

この例においては、ソースとしてのDVDプレーヤ1が、そのEEPROM27に、service_key、hash関数、および疑

似乱数発生関数pRNGを記憶している。これらは、著作権者から与えられたものであり、秘密裡に保管される。また、シンクとしてのパーソナルコンピュータ2のEEPROM 50には、著作権者から与えられたID、LK、LK'、関数G、および疑似乱数発生関数pRNGを有している。

【0073】LKは、著作権者が作成したユニークな乱数であり、LK'は、次式を満足するように生成されている。

$$LK' = G^{-1}(R)$$

$$R = \text{pRNG}(H) \quad (+) \quad \text{pRNG}(LK)$$

$$H = \text{hash}(ID \parallel \text{service_key})$$

【0074】なお、 G^{-1} は、Gの逆関数を意味する。 G^{-1} は、所定の規則を知っていれば、簡単に計算することができるが、知らない場合には、計算することが難しいような特徴を有している。このような関数としては、公開鍵暗号に用いられている関数を利用することができる。

【0075】また、疑似乱数発生関数は、ハードウェアとして設けるようにすることも可能である。

【0076】DVDプレーヤ1のファームウェア20は、最初にステップS101において、パーソナルコンピュータ2のライセンスマネージャ62に対してIDを要求する。パーソナルコンピュータ2のライセンスマネージャ62は、ステップS102でID要求信号を受け取ると、EEPROM50に記憶されているIDを読み出し、ステップS103で、これをDVDプレーヤ1に伝送する。DVDプレーヤ1のファームウェア20は、ステップS104でこのIDを受け取ると、ステップS105で次式を演算する。*

$$\begin{aligned} sk' &= e \quad (+) \quad G(LK') \quad (+) \quad \text{pRNG}(LK) \\ &= sk \quad (+) \quad \text{pRNG}(H) \quad (+) \quad R \quad (+) \quad \text{pRNG}(LK) \\ &= sk \quad (+) \quad \text{pRNG}(H) \quad (+) \quad \text{pRNG}(H) \quad (+) \quad \text{pRNG}(LK) \quad (+) \\ &\quad \text{pRNG}(LK) \\ &= sk \end{aligned}$$

【0084】このようにして、ソースとしてのDVDプレーヤ1とシンクとしてのパーソナルコンピュータ2は、同一の鍵sk、sk'を共有することができる。LK、LK'を作ることができるのは、著作権者だけであるので、ソースが不正に、LK、LK'を作ろうとしても作ることができないので、より安全性を高めることができる。

【0085】以上においては、ソースとシンクにおいて認証を行うようにしたが、例えばパーソナルコンピュータ2には、通常、任意のアプリケーションプログラムをロードして用いることができる。そして、このアプリケーションプログラムとしては、不正に作成したものが使用される場合もある。従って、各アプリケーションプログラム毎に、著作権者から許可を得たものであるか否かを判定する必要がある。そこで、図3に示すように、各アプリケーション部61とライセンスマネージャ62との間においても、上述したように、認証処理を行うようにソースとシンクとの場合、ライセンスマネージャ

$$* H = \text{hash}(ID \parallel \text{service_key})$$

【0077】さらに、ファームウェア20は、ステップS106で鍵skを生成し、ステップS107で次式を演算する。

$$e = sk \quad (+) \quad \text{pRNG}(H)$$

【0078】なお、A (+) Bは、AとBの排他的論理和の演算を意味する。

【0079】すなわち、疑似ランダム発生キーpRNGにステップS105で求めたHを入力することで得られた結果、pRNG(H)と、ステップS106で生成した鍵skのビット毎の排他的論理和を演算することで、鍵SKを暗号化する。

【0080】次に、ステップS108で、ファームウェア20は、eをパーソナルコンピュータ2に伝送する。

【0081】パーソナルコンピュータ2においては、ステップS109でこれを受信し、ステップS110で、次式を演算する。

$$sk' = e \quad (+) \quad G(LK') \quad (+) \quad \text{pRNG}(LK)$$

【0082】すなわち、DVDプレーヤ1から伝送されてきたe、EEPROM50に記憶されている関数Gに、やはりEEPROM50に記憶されているLK'を適用して得られる値G(LK')、並びに、EEPROM50に記憶されているLK'を、やはりEEPROM50に記憶されている疑似乱数発生関数pRNGに適用して得られる結果pRNG(LK)の排他的論理和を演算し、鍵sk'を得る。

【0083】ここで、次式に示すように、sk=sk'となる。

62がソースとなり、アプリケーション部61がシンクとなる。

【0086】次に、以上のようにして、認証が行われた後（暗号鍵の共有が行われた後）、暗号鍵を用いて、ソースから暗号化したデータをシンクに転送し、シンクにおいて、この暗号化したデータを復号する場合の動作について説明する。

【0087】図10に示すように、DVDプレーヤ1、あるいは光磁気ディスク装置3のように、内部の機能が一般ユーザに解放されていない装置においては、1394バス11を介して授受されるデータの暗号化と復号の処理は、それぞれ1394インタフェース26または1394インタフェース36で行われる。この暗号化と復号化には、セッションキーSと時変キーiが用いられるが、このセッションキーSと時変キーi（正確には、時変キーiを生成するためのキーi'）は、それぞれファームウェア20またはファームウェア30から、139

4インタフェース26または1394インタフェース36に供給される。セッションキーSは、初期値として用いられる初期値キーSsと時変キーiを攪乱するために用いられる攪乱キーSiとにより構成されている。この初期値キーSsと攪乱キーSiは、上述した認証において生成された暗号鍵sk(=sk')の所定のビット数の上位ビットと下位ビットにより、それぞれ構成するようにすることができる。このセッションキーSは、セッション毎に、

(例えば、1つの映画情報毎に、あるいは、1回の再生毎に)、適宜、更新される。これに対して、攪乱キーSiとキーi'から生成される時変キーiは、1つのセッション内において、頻繁に更新されるキーであり、例えば、所定のタイミングにおける時刻情報などを用いることができる。

【0088】いま、ソースとしてのDVDプレーヤ1から再生出力した映像データを1394バス11を介して光磁気ディスク装置3とパーソナルコンピュータ2に伝送し、それぞれにおいて復号するものとする。この場合、DVDプレーヤ1においては、1394インタフェース26において、セッションキーSと時変キーiを用いて暗号化処理が行われる。光磁気ディスク装置3においては、1394インタフェース36において、セッションキーSと時変キーiを用いて復号処理が行われる。

【0089】これに対して、パーソナルコンピュータ2においては、ライセンスマネージャ62が、セッションキーSのうち、初期値キーSsをアプリケーション部61に供給し、攪乱キーSiと時変キーi(正確には、時変キーiを生成するためのキーi')を1394インタフェース49(リンク部分)に供給する。そして、1394インタフェース49において、攪乱キーSiとキーi'から時変キーiが生成され、時変キーiを用いて復号が行われ、その復号されたデータをアプリケーション部61において、さらにセッションキーS(正確には、初期値キーSs)を用いて復号が行われる。

【0090】このように、パーソナルコンピュータ2においては、内部バス51が、ユーザに解放されているので、1394インタフェース49により第1段階の復号だけを行い、まだ暗号の状態としておく。そして、アプリケーション部61において、さらに第2段階の復号を行い、平文にする。これにより、パーソナルコンピュータ2に対して、適宜、機能を付加して、内部バス51において授受されるデータ(平文)をハードディスク47や他の装置にコピーすることを禁止させる。

【0091】このように、この発明の実施の形態においては、内部バスが解放されていないCE装置においては、暗号化、または復号処理は、セッションキーSと時変キーiを用いて1度に行われるが、内部バスが解放されている装置(パーソナルコンピュータ2など)においては、復号処理が、時変キーiを用いた復号処理と、セッションキーSを用いた復号処理に分けて行われる。この

ように、1段階の復号処理と、2段階に分けた復号処理の両方ができるようにするには、次式を成立させることが必要となる。

Dec(S, Dec(i, Enc(algo(S+i), Data))) = Data

【0092】なお、上記式において、algo(S+i)は、所定のアルゴリズムにセッションキーSと時変キーiを入力して得られた結果を表している。

【0093】図11は、上記式を満足する1394インタフェース26の構成例を表している。この構成例においては、アディティブジェネレータ71により生成したmビットのデータが、シュリンクジェネレータ73に供給されている。また、LFSR(Linear Feedback Shift Register)72が1ビットのデータを出力し、シュリンクジェネレータ73に供給している。シュリンクジェネレータ73は、LFSR72の出力に対応して、アディティブジェネレータ71の出力を選択し、選択したデータを暗号鍵として加算器74に出力している。加算器74は、入力された平文(1394バス11に伝送するmビットのデータ)と、シュリンクジェネレータ73より供給されるmビットのデータ(暗号鍵)とを加算し、加算した結果を暗号文(暗号化されたデータ)として、1394バス11に出力するようになされている。

【0094】加算器74の加算処理は、 $\text{mod } 2^m$ (\wedge はべき乗を意味する)で、シュリンクジェネレータ73の出力と平文を加算することを意味する。換言すれば、mビットのデータ同士が加算され、キャリオーバを無視した加算値が出力される。

【0095】図12は、図11に示した1394インタフェース26のさらにより詳細な構成例を表している。ファームウェア20から出力されたセッションキーSのうち、初期値キーSsは、加算器81を介してレジスタ82に転送され、保持される。この初期値キーSsは、例えば、55ワード(1ワードは8ビット乃至32ビットの幅を有する)により構成される。また、ファームウェア20から供給されたセッションキーSのうちの、例えばLSB側の32ビットで構成される攪乱キーSiは、レジスタ85に保持される。

【0096】レジスタ84には、キーi'が保持される。このキーi'は、例えば1394バス11を介して1個のパケットが伝送される毎に、2ビットのキーi'がレジスタ84に供給され、16パケット分の(32ビット分の)キーi'がレジスタ84に保持されたとき、加算器86により、レジスタ85に保持されている32ビットの攪乱キーSiと加算され、最終的な時変キーiとして加算器81に供給される。加算器81は、そのときレジスタ82に保持されている値と加算器86より供給された時変キーiを加算し、その加算結果をレジスタ82に供給し、保持させる。

【0097】レジスタ82のワードのビット数が、例え

ば8ビットである場合、加算器86より出力される時変キー i が32ビットであるので、時変キー i を4分割して、各8ビットをレジスタ82の所定のアドレス(0乃至54)のワードに加算するようにする。

【0098】このようにして、レジスタ82には、最初に初期値キー Ss が保持されるが、その後、この値は、16パケット分の暗号文を伝送する毎に、時変キー i で更新される。

【0099】加算器83は、レジスタ82に保持されている55ワードのうちの所定の2ワード(図12に示されているタイミングの場合、アドレス23とアドレス54のワード)を選択し、その選択した2ワードを加算して、シュリンクジェネレータ73に出力する。また、この加算器73の出力は、図12に示すタイミングでは、レジスタ82のアドレス0に転送され、前の保持値に代えて保持される。

【0100】そして、次のタイミングにおいては、加算器83に供給されるレジスタ82の2ワードのアドレスは、アドレス54とアドレス23から、それぞれアドレス53とアドレス22に、1ワード分だけ、図中上方に移動され、加算器83の出力で更新されるアドレスも、図中、より上方のアドレスに移動される。ただし、アドレス0より上方のアドレスは存在しないので、この場合には、アドレス54に移動する。

【0101】なお、加算器81、83、86では、排他的論理和を演算させるようにすることも可能である。

【0102】LFSR72は、例えば、図13に示すように、 n ビットのシフトレジスタ101と、シフトレジスタ101の n ビットのうちの所定のビット(レジスタ)の値を加算する加算器102により構成されている。シフトレジスタ101は、加算器102より供給されるビットを、図中最も左側のレジスタ b_n に保持すると、それまでそこに保持されていたデータを右側のレジスタ b_{n-1} にシフトする。レジスタ b_{n-1} 、 b_{n-2} 、・・・も、同様の処理を行う。そして、さらに次のタイミングでは、各ビットの値を加算器102で加算した値を再び、図中最も左側のビット b_n に保持させる。以上の動作が順次繰り返されて、図中最も右側のレジスタ b_1 から出力が1ビットずつ順次出力される。

【0103】図13は、一般的な構成例であるが、例えば、より具体的には、LFSR72を図14に示すように構成することができる。この構成例においては、シフトレジスタ101が31ビットにより構成され、その図中右端のレジスタ b_1 の値と左端のレジスタ b_{31} の値が、加算器102で加算され、加算された結果がレジスタ b_{31} に帰還されるようになされている。

【0104】LFSR72より出力された1ビットのデータが論理1であるとき、条件判定部91は、アディティブジェネレータ71の加算器83より供給された m ビットのデータをそのままFIFO92に転送し、保持させ

る。これに対して、LFSR72より供給された1ビットのデータが論理0であるとき、条件判定部91は、加算器83より供給された m ビットのデータを受け付けず、暗号化処理を中断させる。このようにして、シュリンクジェネレータ73のFIFO92には、アディティブジェネレータ71で生成した m ビットのデータのうち、LFSR72が論理1を出力したタイミングのもののみが選択され、保持される。

【0105】FIFO92により保持した m ビットのデータが、暗号鍵として、加算器74に供給され、伝送されるべき平文のデータ(DVDからの再生データ)に加算されて、暗号文が生成される。

【0106】暗号化されたデータは、DVDプレーヤ1から1394バス11を介して光磁気ディスク装置3とパーソナルコンピュータ2に供給される。

【0107】光磁気ディスク装置3は、1394インタフェース36において、1394バス11から受信したデータを復号するために、図15に示すような構成を有している。この構成例においては、シュリンクジェネレータ173にアディティブジェネレータ171の出力する m ビットのデータと、LFSR172が出力する1ビットのデータが供給されている。そして、シュリンクジェネレータ173の出力する m ビットの鍵が、減算器174に供給されている。減算器174は、暗号文からシュリンクジェネレータ173より供給される鍵を減算して、平文を復号する。

【0108】すなわち、図15に示す構成は、図11に示す構成と基本的に同様の構成とされており、図11における加算器74が、減算器174に変更されている点だけが異なっている。

【0109】図16は、図15に示す構成のより詳細な構成例を表している。この構成も、基本的に図12に示した構成と同様の構成とされているが、図12における加算器74が、減算器174に変更されている。その他のアディティブジェネレータ171、LFSR172、シュリンクジェネレータ173、加算器181、レジスタ182、加算器183、レジスタ184、185、加算器186、条件判定部191、FIFO192は、図12におけるアディティブジェネレータ71、LFSR72、シュリンクジェネレータ73、加算器81、レジスタ82、加算器83、レジスタ84、85、加算器86、条件判定部91、およびFIFO92に対応している。

【0110】従って、その動作は、基本的に図12に示した場合と同様であるので、その説明は省略するが、図16の例においては、シュリンクジェネレータ173のFIFO192より出力された m ビットの鍵が、減算器174において、暗号文から減算されて平文が復号される。

【0111】以上のように、1394インタフェース36においては、セッションキー S (初期値キー Ss と攪乱

キー S_i)と時変キー i を用いて、暗号化データが1度に復号される。

【0112】これに対して、上述したように、パーソナルコンピュータ2においては、1394インタフェース49とアプリケーション部61において、それぞれ個別に、2段階に分けて復号が行われる。

【0113】図17は、1394インタフェース49において、ハード的に復号を行う場合の構成例を表しており、その基本的構成は、図15に示した場合と同様である。すなわち、この場合においても、アディティブジェネレータ271、LFSR272、シュリンクジェネレータ273、および減算器274により1394インタフェース49が構成されており、これらは、図15におけるアディティブジェネレータ171、LFSR172、シュリンクジェネレータ173、および減算器174と基本的に同様の構成とされている。ただし、図17の構成例においては、アディティブジェネレータ271に対して、ライセンスマネージャ62から、時変キー i を生成するためのキー i' と、セッションキー S のうち、時変キー i を攪乱するための攪乱キー S_i としては、図15における場合と同様のキーが供給されるが、初期値キー S_s としては、全てのビットが0である単位元が供給される。

【0114】すなわち、図18に示すように、初期値キー S_s の全てのビットが0とされるので、実質的に、初期値キー S_s が存在しない場合と同様に、時変キー i だけに基づいて暗号鍵が生成される。その結果、減算器274においては、暗号文の時変キー i に基づく復号だけが行われる。まだ初期値キー S_s に基づく復号が行われていないので、この復号の結果得られるデータは、完全な平文とはなっておらず、暗号文の状態になっている。従って、このデータを内部バス51から取り込み、ハードディスク47や、その他の記録媒体に記録したとしても、それをそのまま利用することができない。

【0115】そして、以上のようにして、1394インタフェース49において、ハード的に時変キー i に基づいて復号されたデータをソフト的に復号するアプリケーション部61の構成は、図19に示すように、アディティブジェネレータ371、LFSR372、シュリンクジェネレータ373および減算器374により構成される。その基本的構成は、図15に示したアディティブジェネレータ171、LFSR172、シュリンクジェネレータ173、および減算器174と同様の構成となっている。

【0116】ただし、セッションキー S のうち、初期値キー S_s は、図15における場合と同様に、通常の初期値キーが供給されるが、時変キー i を生成するための攪乱キー S_i とキー i' は、それぞれ全てのビットが0である単位元のデータとされる。

【0117】その結果、図20にその詳細を示すように(そのアディティブジェネレータ371乃至FIFO392は、図16におけるアディティブジェネレータ171乃至

至FIFO192に対応している)、レジスタ384に保持されるキー i' とレジスタ385に保持される攪乱キー S_i は、全てのビットが0であるため、加算器386の出力する時変キー i も全てのビットが0となり、実質的に時変キー i が存在しない場合と同様の動作が行われる。すなわち、初期値キー S_s だけに基づく暗号鍵が生成される。そして、減算器374においては、このようにして生成された暗号鍵に基づいて暗号文が平文に復号される。上述したように、この暗号文は、1394インタフェース49において、時変キー i に基づいて第1段階の復号が行われているものであるので、ここで、初期値キー S_s に基づいて第2段階の復号を行うことで、完全な平文を得ることができる。

【0118】光磁気ディスク装置3においては、以上のようにして暗号文が復号されると、CPU31が、復号されたデータをドライブ35に供給し、光磁気ディスクに記録させる。

【0119】一方、パーソナルコンピュータ2においては、CPU41(アプリケーション部61)が、以上のようにして復号されたデータを、例えばハードディスク47に供給し、記録させる。パーソナルコンピュータ2においては、拡張ボード48として所定のボードを接続して、内部バス51で授受されるデータをモニタすることができるが、内部バス51に伝送されるデータを最終的に復号することができるのは、アプリケーション部61であるので、拡張ボード48は、1394インタフェース49で、時変キー i に基づく復号が行われたデータ(まだ、セッションキー S に基づく復号が行われていないデータ)をモニタすることができたとしても、完全に平文に戻されたデータをモニタすることはできない。そこで、不正なコピーが防止される。

【0120】なお、セッションキーの共有は、例えば、Diffie-Hellman法などを用いて行うようにすることも可能である。

【0121】なお、この他、例えばパーソナルコンピュータ2における1394インタフェース49またはアプリケーション部61の処理能力が比較的低く、復号処理を行うことができない場合には、セッションキーと時変キーのいずれか、あるいは両方をソース側において、単位元で構成するようにし、シンク側においても、これらを単位元で用いるようにすれば、実施的にセッションキーと時変キーを使用しないで、データの授受が可能となる。ただし、そのようにすれば、データが不正にコピーされるおそれが高くなる。

【0122】アプリケーション部61そのものが、不正にコピーしたものである場合、復号したデータが不正にコピーされてしまう恐れがあるが、上述したようにアプリケーション部61をライセンスマネージャ62で認証するようにすれば、これを防止することが可能である。

【0123】この場合の認証方法としては、共通鍵暗号

方式の他、公開鍵暗号方式を用いたデジタル署名を利用することができる。

【0124】以上の図11、図12、図15乃至図20に示す構成は、準同形(homomorphism)の関係を満足するものとなっている。すなわち、キー K_1 、 K_2 がガロアフィールド G の要素であるとき、両者の群演算の結果、 $K_1 \cdot K_2$ もガロアフィールド G の要素となる。そして、さらに、所定の関数 H について次式が成立する。

$$H(K_1 \cdot K_2) = H(K_1) \cdot H(K_2)$$

【0125】図21は、さらに1394インタフェース26の他の構成例を表している。この構成例においては、セッションキー S がLFSR501乃至503に供給され、初期設定されるようになされている。LFSR501乃至503の幅 n_1 乃至 n_3 は、それぞれ20ビット程度で、それぞれの幅 n_1 乃至 n_3 は、相互に素になるように構成される。従って、例えば、セッションキー S のうち、例えば、上位 n_1 ビットがLFSR501に初期設定され、次の上位 n_2 ビットがLFSR502に初期設定され、さらに次の上位 n_3 ビットがLFSR503に初期設定される。

【0126】LFSR501乃至503は、クロッキングファンクション506より、例えば論理1のイネーブル信号が入力されたとき、 m ビットだけシフト動作を行い、 m ビットのデータを出力する。 m の値は、例えば、8、16、32、40などとしてすることができる。

【0127】LFSR501とLFSR502の出力は、加算器504に入力され、加算される。加算器504の加算値のうち、キャリー成分は、クロッキングファンクション506に供給され、sum成分は、加算器505に供給され、LFSR503の出力と加算される。加算器505のキャリー成分は、クロッキングファンクション506に供給され、sum成分は、排他的論理和回路508に供給される。

【0128】クロッキングファンクション506は、加算器504と加算器505より供給されるデータの組み合わせが、00、01、10、11のいずれかであるので、これらに対応して、LFSR501乃至503に対して、000乃至111のいずれか1つの組み合わせのデータを出力する。LFSR501乃至503は、論理1が入力されたとき、 m ビットのシフト動作を行い、新たな m ビットのデータを出力し、論理0が入力されたとき、前回出力した場合と同一の m ビットのデータを出力する。

【0129】排他的論理和回路508は、加算器505の出力するsum成分とレジスタ507に保持された時変キー i の排他的論理和を演算し、その演算結果を排他的論理和回路509に出力する。排他的論理和回路509は、入力された平文と、排他的論理和回路508より入力された暗号鍵の排他的論理和を演算し、演算結果を暗号文として出力する。

【0130】図22は、光磁気ディスク装置3における

1394インタフェース36の構成例を表している。この構成例におけるLFSR601乃至排他的論理和回路609は、図21におけるLFSR501乃至排他的論理和回路509と同様の構成とされている。従って、その動作も、基本的に同様となるので、その説明は省略する。ただし、図21の構成例においては、暗号化処理が行われるのに対して、図22の構成例においては、復号処理が行われる。

【0131】図23は、パーソナルコンピュータ2の1394インタフェース49の構成例を表している。この構成例におけるLFSR701乃至排他的論理和回路709も、図22における、LFSR601乃至排他的論理和回路609と同様の構成とされている。ただし、LFSR701乃至703に初期設定されるセッションキー S は、全てのビットが0の単位元とされている。従って、この場合、実質的にレジスタ707に保持された時変キー i だけに対応して復号化処理が行われる。

【0132】図24は、パーソナルコンピュータ2のアプリケーション部61の構成例を表している。この構成例におけるLFSR801乃至排他的論理和回路809は、図22における、LFSR601乃至排他的論理和回路609と基本的に同様の構成とされている。ただし、レジスタ807に入力される時変キー i が、全てのビットが0である単位元とされている点のみが異なっている。従って、この構成例の場合、セッションキー S だけに基いて暗号鍵が生成され、復号処理が行われる。

【0133】なお、図19、図20、および図24に示す処理は、アプリケーション部61において行われるので、ソフト的に処理されるものである。

【0134】以上においては、DVDプレーヤ1をソースとし、パーソナルコンピュータ2と光磁気ディスク装置3をシンクとしたが、いずれの装置をソースとするかシンクとするかは任意である。

【0135】また、各電子機器を接続する外部バスも、1394バスに限らず、種々のバスを利用することができる。それに接続する電子機器も、上述した例に限らず、任意の装置とすることができる。

【0136】

【発明の効果】以上の如く、請求項1に記載の暗号化装置および請求項9に記載の暗号化方法によれば、第1の鍵と、データを暗号化しているとき、所定のタイミングで変更される第2の鍵を用いて暗号鍵を生成するようにしたので、より安全に暗号化を行うことが可能となる。

【0137】請求項10に記載の復号装置および請求項13に記載の復号方法によれば、第1の鍵と、データを復号しているとき、所定のタイミングで変更される第2の鍵を用いて暗号鍵を生成するようにしたので、より安全に暗号化されているデータを復号することが可能となる。

【0138】請求項14に記載の情報処理システムおよび

び請求項 15 に記載の情報処理方法によれば、機能の変更がユーザに開放されていない第 1 の情報処理装置においては、第 1 の鍵と、データを復号しているとき、所定のタイミングで変更される第 2 の鍵を用いて、暗号鍵を生成するようにし、機能の変更がユーザに開放されている第 2 の情報処理装置においては、第 1 の鍵と、第 2 の鍵の一方を用いて生成した第 1 の暗号鍵で、暗号化されているデータを復号し、第 1 の鍵と第 2 の鍵の他方を用いて生成した第 2 の暗号鍵を用いて、その復号されたデータをさらに復号するようにしたので、より安全な情報処理システムを実現することが可能となる。

【0139】請求項 16 に記載の情報処理装置および請求項 17 に記載の情報処理方法によれば、第 1 の暗号鍵と、データを復号しているとき、所定のタイミングで変更される第 2 の暗号鍵を、ソフトウェアプログラムで生成するようにしたので、アプリケーションプログラム毎に復号を行うことが可能となり、不正なコピーをより確実に防止することが可能となる。

【図面の簡単な説明】

【図 1】本発明を適用した情報処理システムの構成例を示すブロック図である。

【図 2】図 1 の DVD プレーヤ 1、パーソナルコンピュータ 2、および光磁気ディスク装置 3 の内部の構成例を示すブロック図である。

【図 3】認証処理を説明する図である。

【図 4】認証処理を説明するタイミングチャートである。

【図 5】node_unique_ID のフォーマットを示す図である。

【図 6】他の認証処理を説明するタイミングチャートである。

【図 7】さらに他の認証処理を説明するタイミングチャートである。

【図 8】他の認証処理を説明するタイミングチャートである。

【図 9】他の認証処理を説明するタイミングチャートである。

【図 10】暗号化処理を説明するブロック図である。

【図 11】図 10 の 1394 インタフェース 26 の構成

例を示すブロック図である。

【図 12】図 11 の 1394 インタフェース 26 のより詳細な構成例を示すブロック図である。

【図 13】図 12 の LFSR 72 のより詳細な構成例を示すブロック図である。

【図 14】図 13 の LFSR 72 のより具体的な構成例を示すブロック図である。

【図 15】図 10 の 1394 インタフェース 36 の構成例を示すブロック図である。

【図 16】図 15 の 1394 インタフェース 36 のより詳細な構成例を示すブロック図である。

【図 17】図 10 の 1394 インタフェース 49 の構成例を示すブロック図である。

【図 18】図 17 の 1394 インタフェース 49 のより詳細な構成例を示すブロック図である。

【図 19】図 10 のアプリケーション部 61 の構成例を示すブロック図である。

【図 20】図 19 のアプリケーション部 61 のより詳細な構成例を示すブロック図である。

【図 21】図 10 の 1394 インタフェース 26 の他の構成例を示すブロック図である。

【図 22】図 10 の 1394 インタフェース 36 の他の構成例を示すブロック図である。

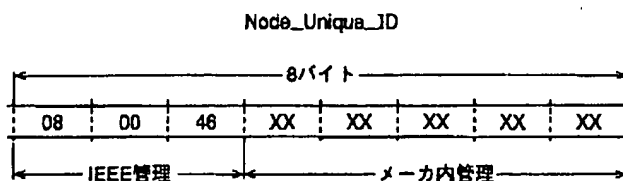
【図 23】図 10 の 1394 インタフェース 49 の他の構成例を示すブロック図である。

【図 24】図 10 のアプリケーション部 61 の他の構成例を示すブロック図である。

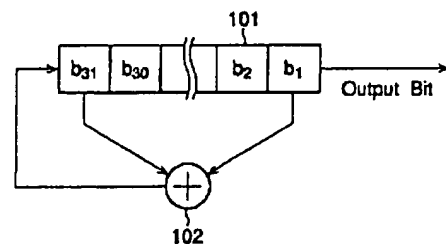
【符号の説明】

1 DVDプレーヤ, 2 パーソナルコンピュータ,
3 光磁気ディスク装置, 11 1394バス, 20 ファームウェア, 21 CPU, 25 ドライブ,
26 1394インタフェース, 27 EEPROM,
31 CPU, 35 ドライブ, 36 1394インタフェース,
37 EEPROM, 41 CPU, 47 ハードディスク,
48 拡張ボード, 49 1394インタフェース,
50 EEPROM, 51 内部バス,
61 アプリケーション部, 62 ライセンスマネージャ

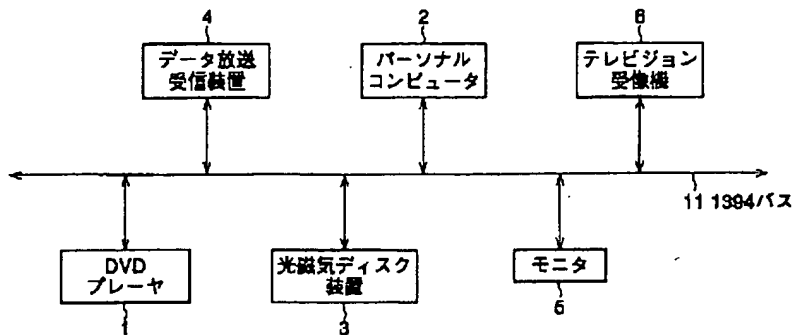
【図 5】



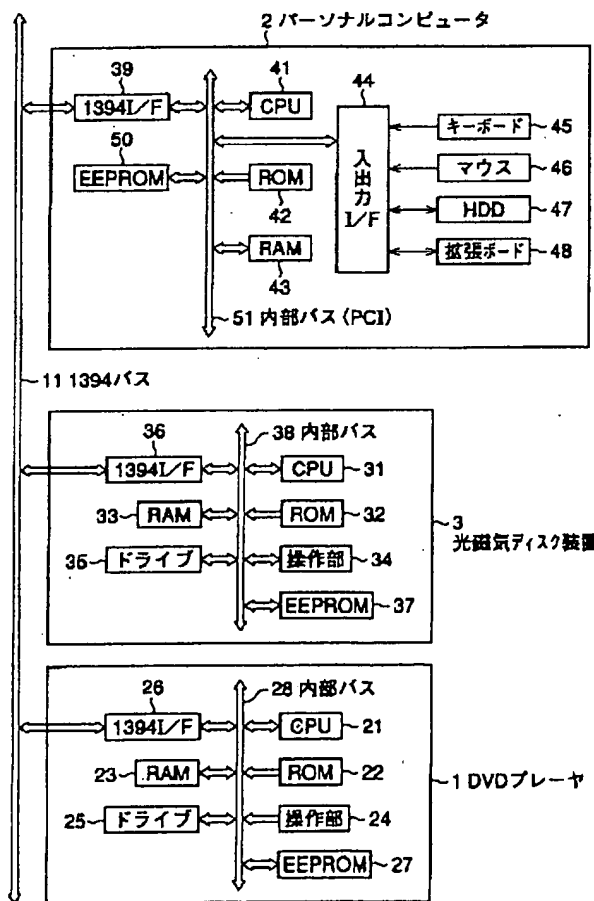
【図 14】



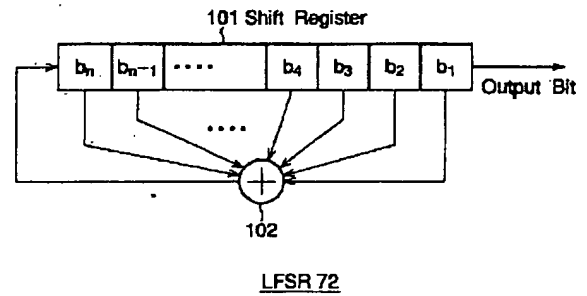
【図1】



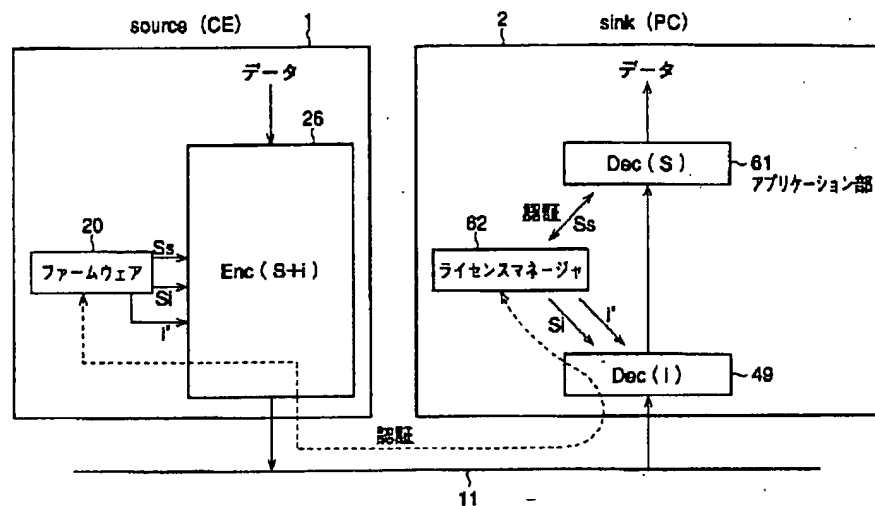
【図2】



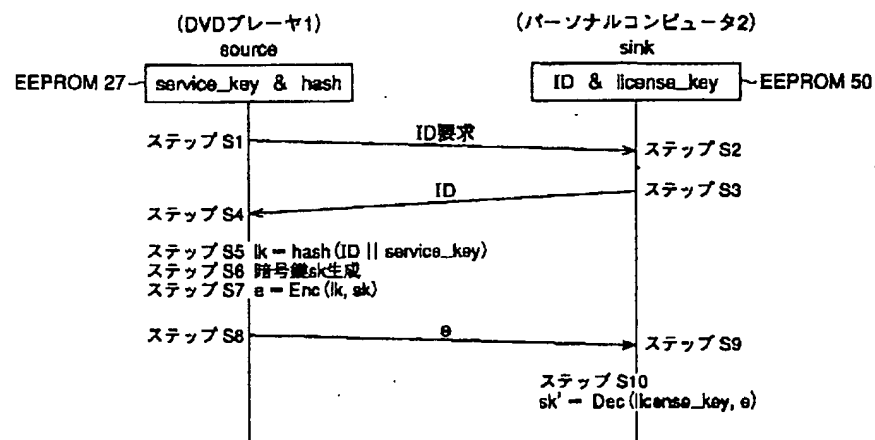
【図13】



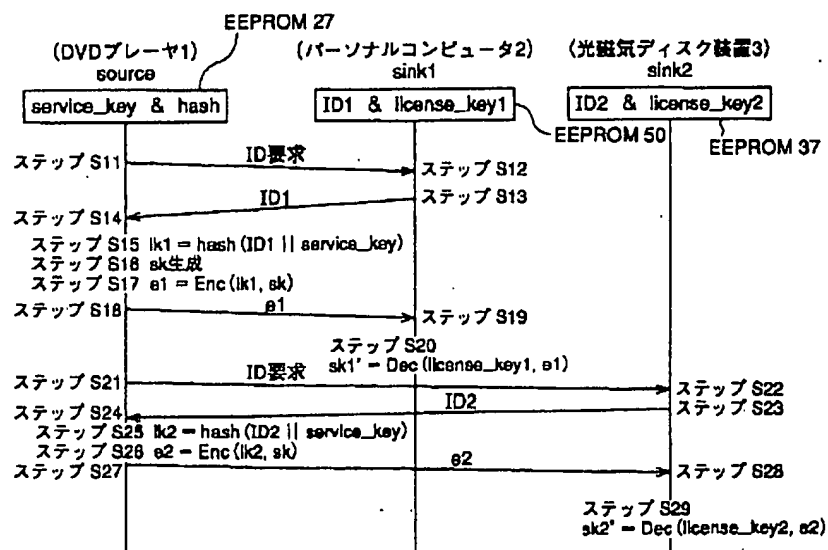
【図3】



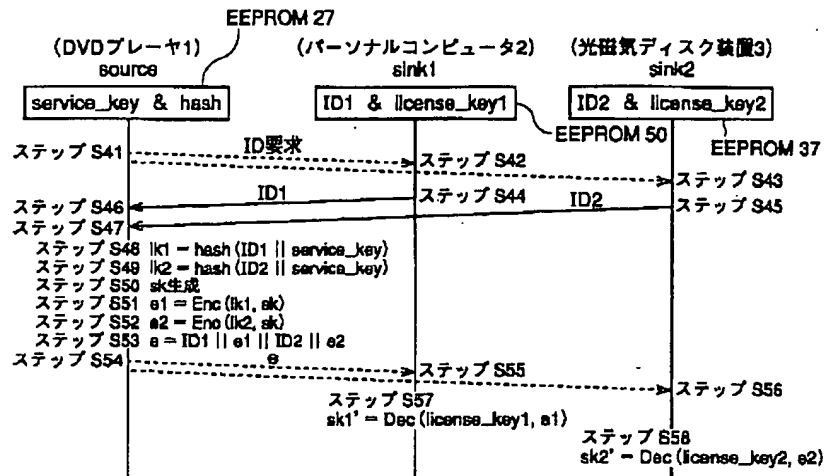
【図4】



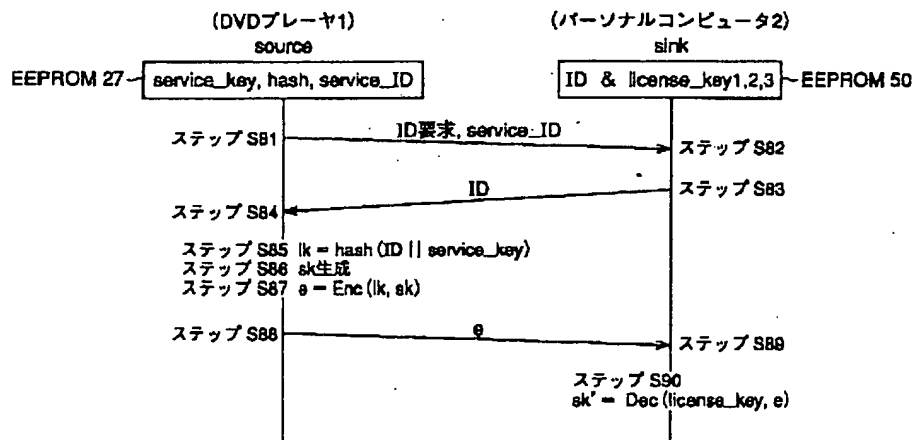
【図6】



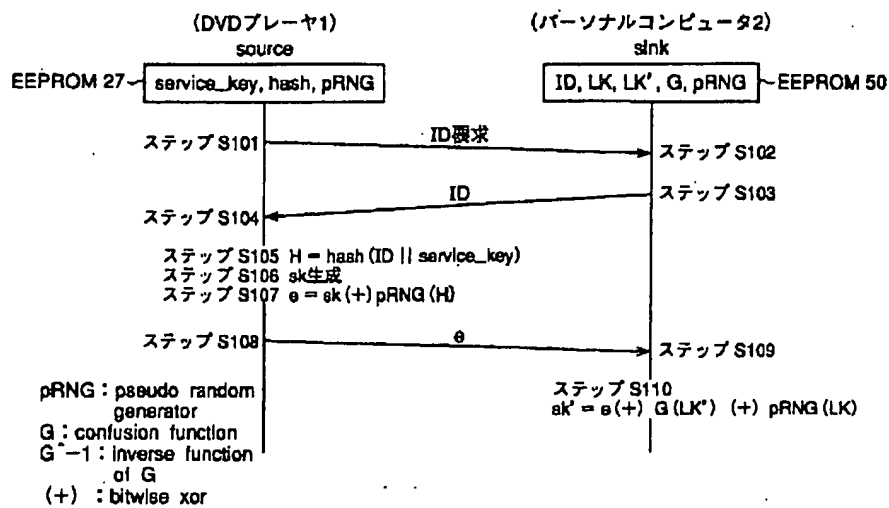
【図7】



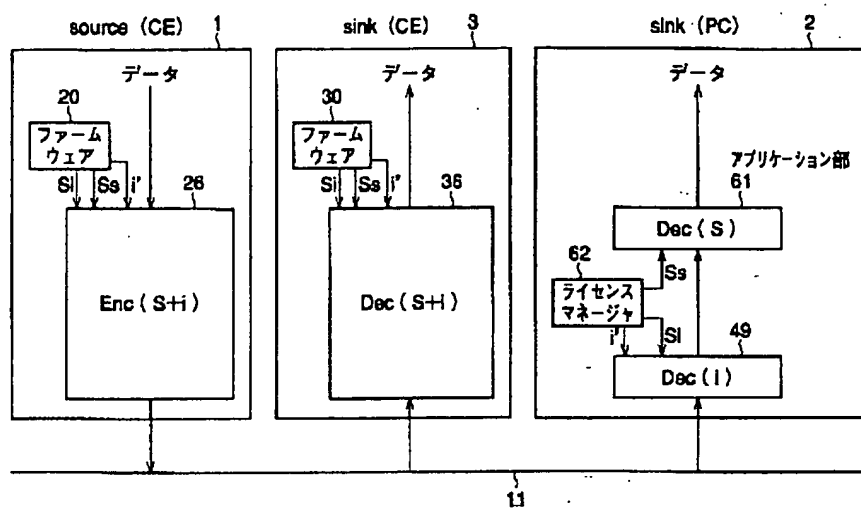
【図8】



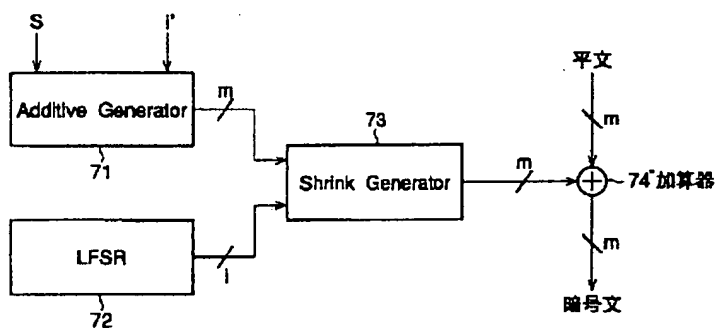
【図9】



【図 10】

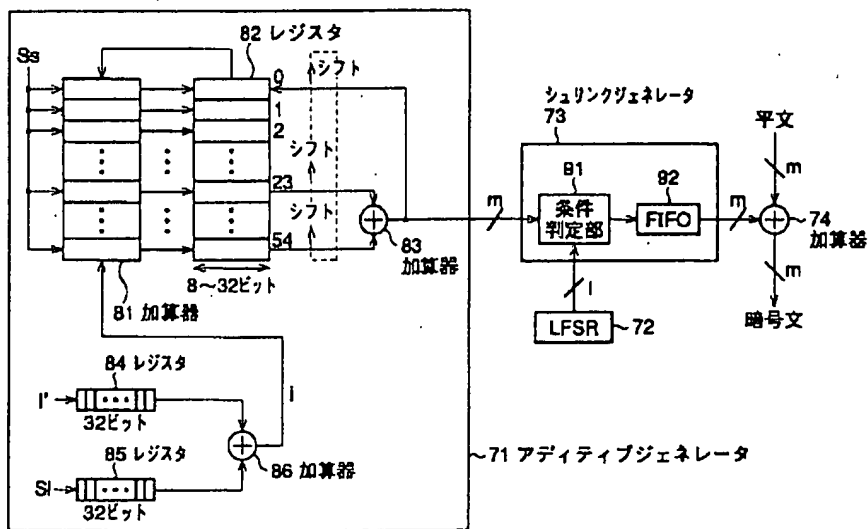


【図 1 1】



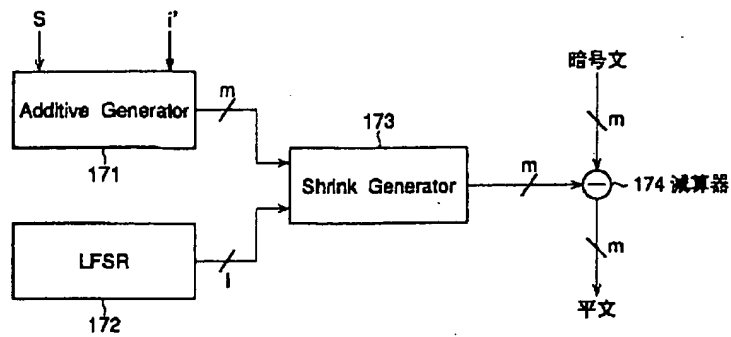
1394I/F 26
(ソース (CE))

【图 12】



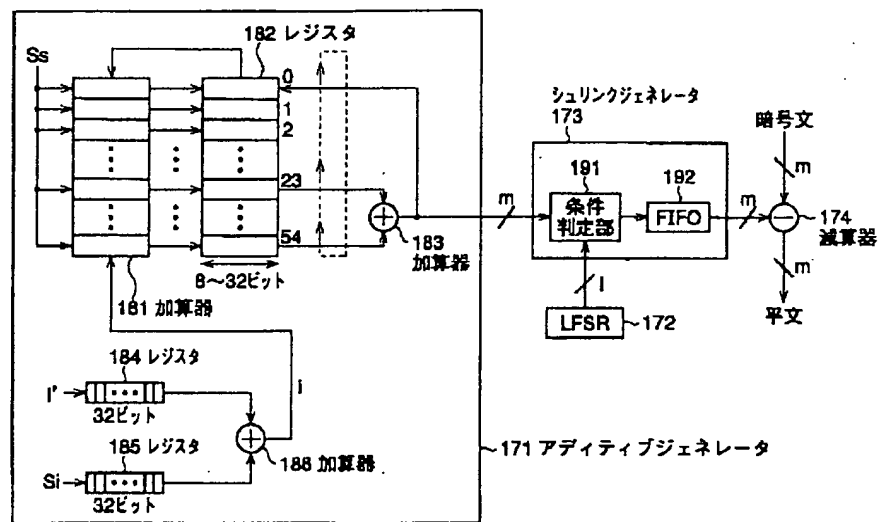
13041/F 26
(ソース (CE))

【図15】



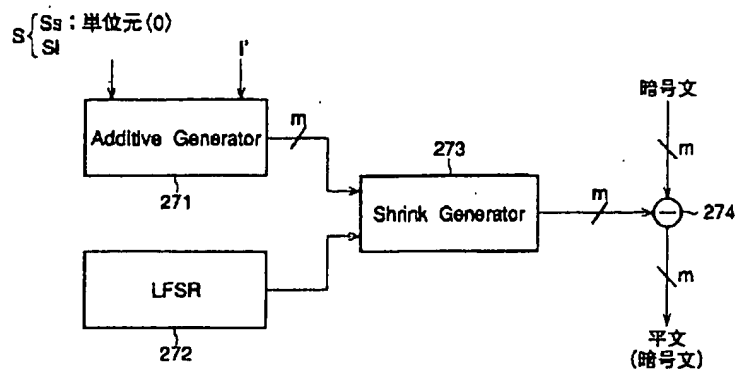
1394I/F 36
(シンク (CE))

【図16】



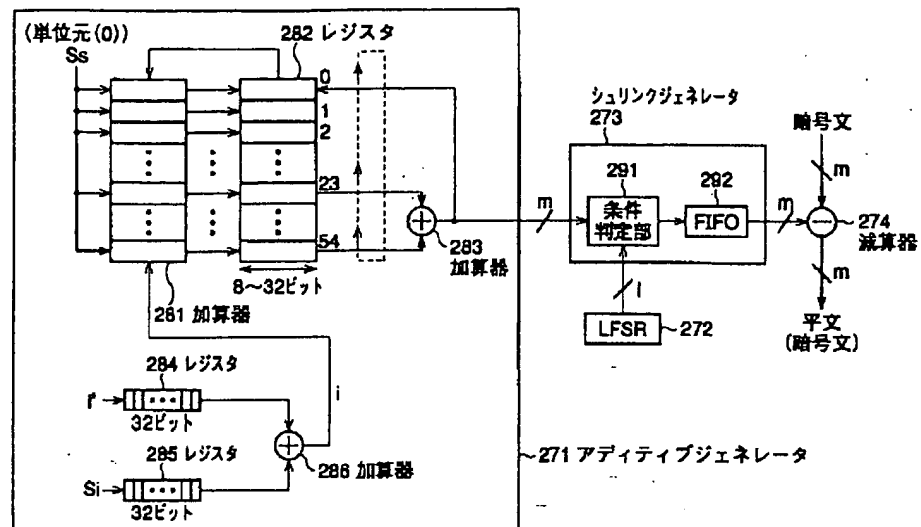
1394I/F 36
(シンク (CE))

【図17】



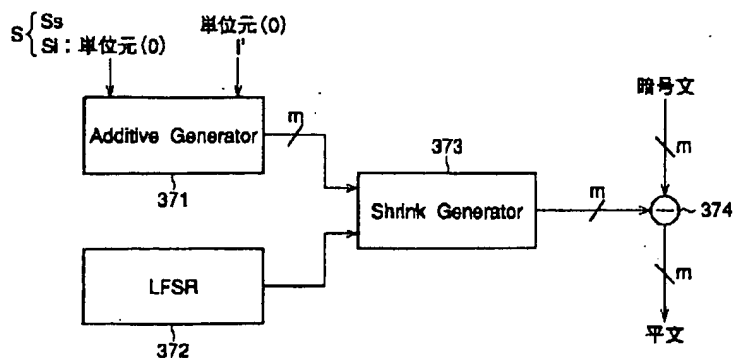
1394I/F 49
(シンク (PC) のリンク部分)

【図18】



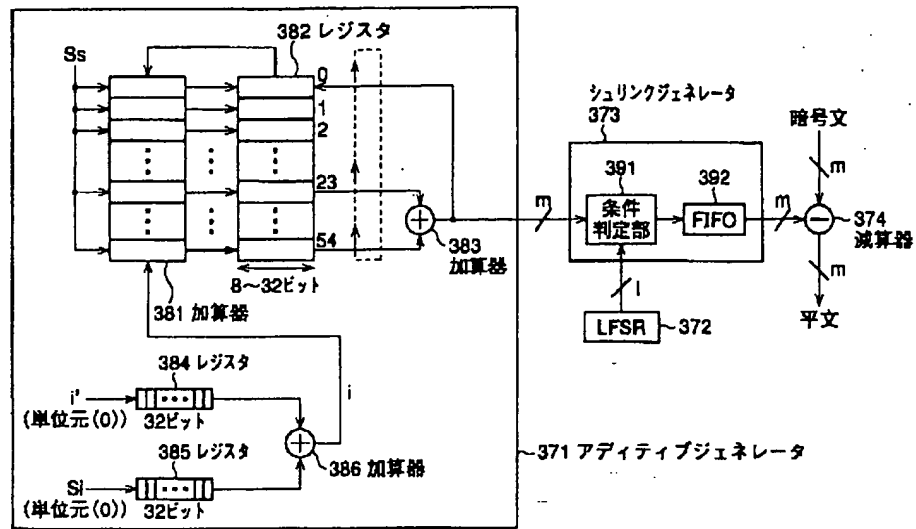
1394L/F 49
(シンク(PC)のリンク部分)

【図19】



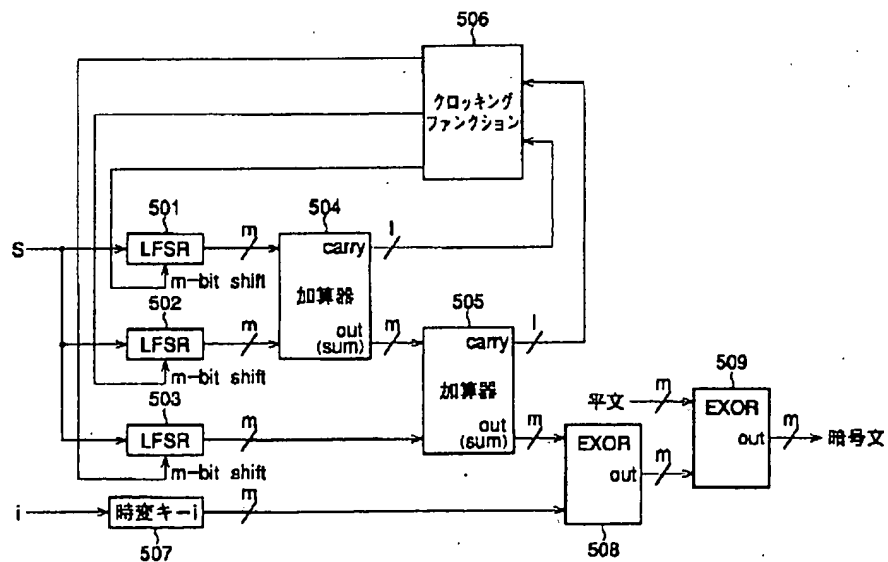
シンク(PC)のアプリケーション部 61

【図 20】

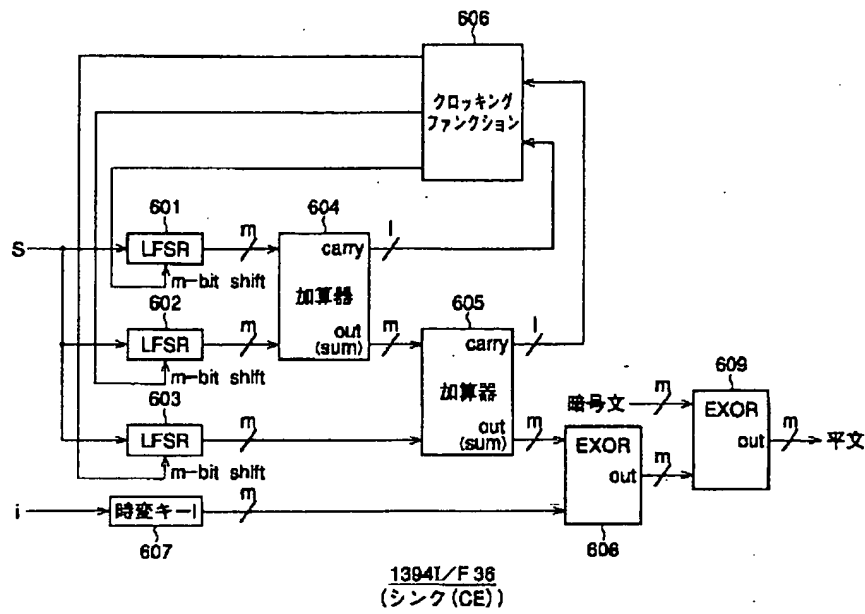


シンク (PC) のアプリケーション部 81

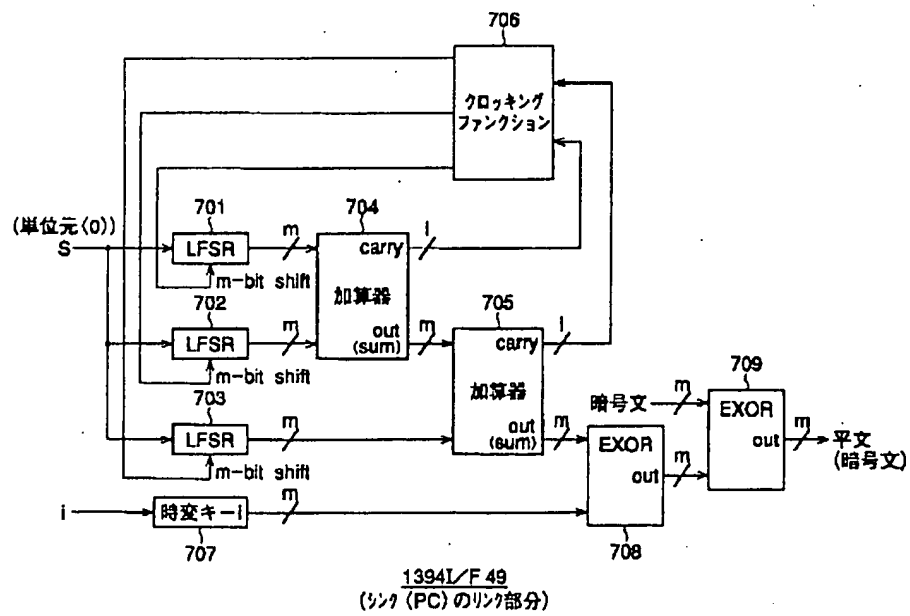
【図 21】

1394L/F 26
(ソース (CE))

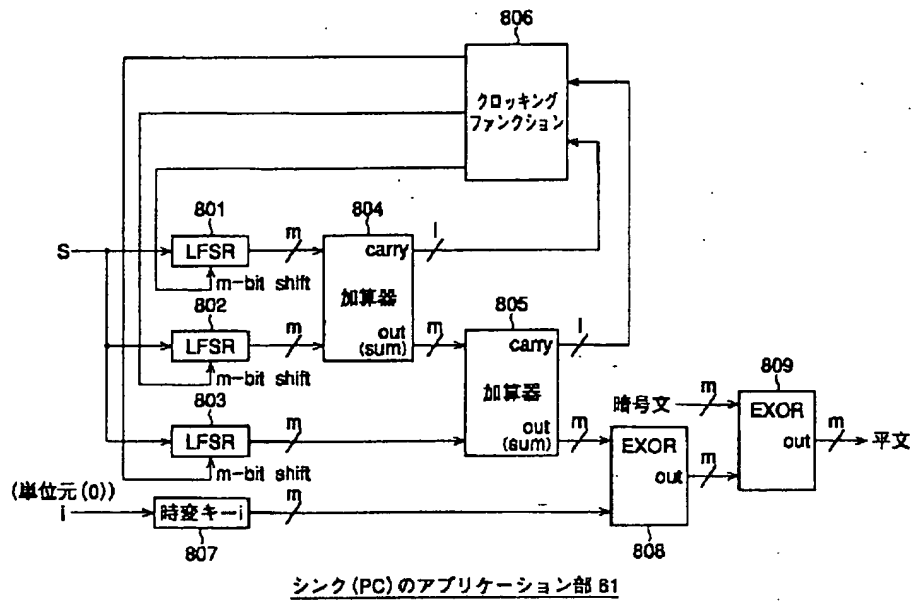
【図 22】



【図 23】



【図24】



フロントページの続き

(72)発明者 佐藤 真
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 嶋 久登
アメリカ合衆国 カリフォルニア州 サラ
トガ パセオ・フローレス12610

(72)発明者 浅野 智之
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.